

took Denial Authority action, or his or her representative, may serve as a non-voting member when the Board considers matters in the Denial Authority's area of functional specialization.

(4) The Board may seek additional information, including the requester's official personnel file, if relevant and necessary to decide the appeal.

(5) If the Board determines that an amendment is warranted (the record is inaccurate as a matter of fact rather than judgment, irrelevant, untimely, or incomplete) it will amend the record and notify the requester, the Denial Authority, the custodian of the record, and any prior recipients of the record, of the amendment.

(6) If the Board determines that amendment is unwarranted, they will—

(i) Obtain the General Counsel's concurrence in writing;

(ii) Respond to the requester with the reasons for denial; and

(iii) Inform the requester of the right to file a "Statement of Disagreement" with the Board's action and to seek judicial review of the Army's refusal to amend. A "Statement of Disagreement" must be received by the system manager within 120 days and it will be made an integral part of the pertinent record. Anyone who may have access to, use of, or need to disclose information from the record will be aware that the record was disputed. The disclosing authority may include a brief summary of the Board's reasons for not amending the disputed record.

(7) It is inappropriate for the Privacy Act Review Board to consider any record which is exempt from the amendment provision of the Privacy Act.

§ 505.7 Disclosure of personal information to other agencies and third parties.

(a) *Disclosing records to third parties.*

(1) DA is prohibited from disclosing a record from a Privacy Act system of records to any person or agency without the prior written consent of the subject of the record, except when—

(i) Pursuant to the twelve Privacy Act exceptions. The twelve exceptions to the "no disclosure without consent" rule are those exceptions which permit

the release of personal information without the individual's/subject's consent (See appendix C of this part).

(ii) The FOIA requires the release of the record. One of the twelve exceptions to Privacy Act is the FOIA Exception. If the FOIA requires the release of information, the information must be released. The Privacy Act can not prevent release to a third party if the FOIA requires release. However, information must not be discretionarily released under the FOIA if the information is subject to the Privacy Act's "no disclosure without consent" rule.

(iii) A routine use applies. Another major exception to the "no disclosure without consent" rule is the routine use exception. The Privacy Act allows federal agencies to publish routine use exceptions to the Privacy Act. Some routine uses are Army specific, DOD specific, and Governmentwide. Routine uses exceptions are listed in the Privacy Act system of records notice(s) applicable to the Privacy Act records in question. The Army and other agencies' system of records notices may be accessed at the Defense Privacy Office's Web site <http://www.defenselink.mil/privacy>.

(2) The approved twelve exceptions to the Privacy Act "no disclosure without consent" rule are listed at appendix C of this part.

(b) *Disclosing records to other DOD components and to federal agencies outside the DOD.* (1) The twelve Privacy Act exceptions referred to in appendix C of this part are available to other DOD components and to federal agencies outside the DOD as exceptions to the Privacy Act's "no disclosure without consent" rule, with the exception of the FOIA exception. The FOIA is not an appropriate mechanism for providing information to other DOD components and to federal agencies outside the DOD.

(2) A widely used exception to requests for information from local and state government agencies and federal agencies not within the DOD is the routine use exception to the Privacy Act.

(3) The most widely used exception to requests for information from other DOD components is the "intra-agency

Department of the Army, DoD

§ 505.7

need to know” exception to the Privacy Act. Officers and employees of the DOD who have an official need for the records in the performance of their official duties are entitled to Privacy Act protected information. Rank, position, or title alone does not authorize access to personal information about others. An official need for the information must exist before disclosure.

(4) For the purposes of disclosure and disclosure accounting, the Department of Defense (DOD) is considered a single agency.

(c) *Disclosures under AR 25-55, the Freedom of Information Act (FOIA) Program.* (1) Despite Privacy Act protections, all records must be disclosed if the Freedom of Information Act (FOIA) requires their release. The FOIA requires release unless the information is exempted by one or more of the nine FOIA exemptions.

(2) Required release under the FOIA. The following are examples of personal information that is generally not exempt from the FOIA; therefore, it must be released to the public, unless covered by paragraphs (d)(2) and (d)(3) of this section. The following list is not all inclusive:

(i) Military Personnel—

(A) Rank, date of rank, active duty entry date, basic pay entry date, and gross pay (including base pay, special pay, and all allowances except Basic Allowance for Housing);

(B) Present and past duty assignments, future stateside assignments;

(C) Office/unit name, duties address and telephone number (DOD policy may require withholding of this information in certain circumstances);

(D) Source of commission, promotion sequence number, military awards and decorations, and professional military education;

(E) Duty status, at any given time;

(F) Separation or retirement dates;

(G) Military occupational specialty (MOS);

(H) Active duty official attendance at technical, scientific or professional meetings; and

(I) Biographies and photos of key personnel (DOD policy may require withholding of this information in certain circumstances).

(ii) Federal civilian employees—

(A) Present and past position titles, occupational series, and grade;

(B) Present and past annual salary rates (including performance awards or bonuses, incentive awards, merit pay amount, Meritorious or Distinguished Executive Ranks, and allowances and differentials);

(C) Present and past duty stations;

(D) Office or duty telephone number (DOD policy may require withholding of this information in certain circumstances); and

(E) Position descriptions, identification of job elements, and performance standards (but not actual performance appraisals), the release of which would not interfere with law enforcement programs or severely inhibit agency effectiveness. Performance elements and standards (or work expectations) may also be withheld when they are so intertwined with performance appraisals, the disclosure would reveal an individual's performance appraisal.

(d) *Personal information that requires protection.* (1) The following are examples of information that is generally NOT releasable without the written consent of the subject. This list is not all inclusive—

(i) Marital status;

(ii) Dependents' names, sex and SSN numbers;

(iii) Civilian educational degrees and major areas of study (unless the request for the information relates to the professional qualifications for Federal employment);

(iv) School and year of graduation;

(v) Home of record;

(vi) Home address and phone;

(vii) Age and date of birth;

(viii) Overseas assignments (present or future);

(ix) Overseas office or unit mailing address and duty phone of routinely deployable or sensitive units;

(x) Race/ethnic origin;

(xi) Educational level (unless the request for the information relates to professional qualifications for federal employment);

(xii) Social Security Number (SSN); and

(xiii) The information that would otherwise be protected from mandatory disclosure under a FOIA exemption.

(2) The Office of the Secretary of Defense issued a policy memorandum in 2001 that provided greater protection of DOD personnel in the aftermath of 9/11 by requiring information that personally identifies DOD personnel be more carefully scrutinized and limited. In general, the Department of Defense has specifically advised that DOD components are not to release lists of names, duty addresses, present or past position titles, grades, salaries, and performance standards of DOD military members and civilian employees. At the office director level or above, the release of information will be limited to the name, official title, organization, and telephone number, provided a determination is made that disclosure does not raise security or privacy concerns. No other information, including room numbers, will normally be released about these officials. Consistent with current policy, information on officials below the office director level may continue to be released if their positions or duties require frequent interaction with the public.

(3) Disclosure of records pertaining to personnel of overseas, sensitive, or routinely deployed units shall be prohibited to the extent authorized by 10 U.S.C. 130b.

(e) *Release of home addresses and home telephone numbers.* (1) The release of home addresses and home telephone numbers normally is prohibited. This release is normally considered a clearly “unwarranted invasion” of personal privacy and is exempt from mandatory release under the FOIA. However, home addresses and home telephone numbers may still be released if—

(i) The individual has indicated previously in writing that he or she has no objection to the release;

(ii) The source of the information to be released is a public document such as commercial telephone directory or other public listing;

(iii) The release is required by Federal statute (for example, pursuant to federally funded state programs to locate parents who have defaulted on child support payments) (See 42 U.S.C. 653); or

(iv) The releasing of information is pursuant to the routine use exception

or the “intra-agency need to know” exception to the Privacy Act.

(2) A request for a home address or telephone number may be referred to the last known address of the individual for a direct reply by the individual to the requester. In such cases, the requester shall be notified of the referral.

(3) Do not sell or rent lists of individual names and addresses unless such action is specifically authorized by the appropriate authority.

(f) *Emergency recall rosters.* (1) The release of emergency recall rosters normally is prohibited. Their release is normally considered a clearly “unwarranted invasion” of personal privacy and is exempt from mandatory release under the FOIA. Emergency recall rosters should only be shared with those who have an “official need to know” the information, and they should be marked “For Official Use Only” (See AR 25–55).

(2) Do not include a person’s SSN on an emergency recall roster or their spouse’s name.

(3) Commanders and supervisors should give consideration to those individuals with unlisted phone numbers. Commanders and supervisors should consider limiting access to an unlisted number within the unit.

(g) *Social rosters.* (1) Before including personal information such as a spouse’s name, home addresses, home phone numbers, and similar information on social rosters or social directories, which will be shared with individuals, always ask for the individual’s written consent. Without their written consent, do not include this information.

(2) Collection of this information will require a Privacy Act Statement which clearly tells the individual what information is being solicited, the purpose, to whom the disclosure of the information is made, and whether collection of the information is voluntary or mandatory.

(h) *Disclosure of personal information on group orders.* (1) Personal information will not be posted on group orders so that everyone on the orders can view it. Such a disclosure of personal information violates the Privacy Act and this part.

Department of the Army, DoD

§ 505.8

(2) The following are some examples of personal information that should not be contained in group orders. The following list is not all-inclusive—

- (i) Complete SSN;
- (ii) Home addresses and phone numbers; or
- (iii) Date of birth.

(i) *Disclosures for established routine uses.* (1) Records may be disclosed outside the DOD without the consent of the individual to whom they pertain for an established routine use.

(2) A routine use shall—

(i) Be compatible with and related to the purpose for which the record was compiled;

(ii) Identify the persons or organizations to which the records may be released; and

(iii) Have been published previously in the FEDERAL REGISTER.

(3) Establish a routine use for each user of the information outside the Department of Defense who needs official access to the records.

(4) Routine uses may be established, discontinued, or amended without the consent of the individuals involved. However, new or changed routine uses must be published in the FEDERAL REGISTER at least 30 days before actually disclosing any records.

(5) In addition to the routine uses listed in the applicable systems of records notices, “Blanket Routine Uses” for all DOD maintained systems of records have been established. These “Blanket Routine Uses” are applicable to every record system maintained within the DOD unless specifically stated otherwise within a particular record system. The “Blanket Routine Uses” are listed at appendix C of this part.

(j) *Disclosure accounting.* (1) System managers must keep an accurate record of all disclosures made from DA Privacy Act system of records, including those made with the consent of the individual, except when records are—

(i) Disclosed to DOD officials who have a “need to know” the information to perform official government duties; or

(ii) Required to be disclosed under the Freedom of Information Act.

(2) The purpose for the accounting of disclosure is to—

(i) Enable an individual to ascertain those persons or agencies that have received information about them;

(ii) Enable the DA to notify past recipients of subsequent amendments or “Statements of Dispute” concerning the record; and

(iii) Provide a record of DA compliance with the Privacy Act of 1974, if necessary.

(3) Since the characteristics of records maintained within DA vary widely, no uniform method for keeping the disclosure accounting is prescribed.

(4) Essential elements to include in each disclosure accounting report are—

(i) The name, position title, and address of the person making the disclosure;

(ii) Description of the record disclosed;

(iii) The date, method, and purpose of the disclosure; and

(iv) The name, position title, and address of the person or agency to which the disclosure was made.

(5) The record subject has the right of access to the disclosure accounting except when—

(i) The disclosure was made for law enforcement purposes under 5 U.S.C. 552a(b)(7); or

(ii) The disclosure was made from a system of records for which an exemption from 5 U.S.C. 552a(c)(3) has been claimed.

(6) There are no approved filing procedures for the disclosure of accounting records; however, system managers must be able to retrieve upon request. With this said, keep disclosure accountings for 5 years after the disclosure, or for the life of the record, whichever is longer.

(7) When an individual requests such an accounting, the system manager or designee will respond within 20 working days.

§ 505.8 Training requirements.

(a) *Training.* (1) The Privacy Act requires all heads of Army Staff agencies, field operating agencies, direct reporting units, Major Commands, subordinate commands, and installations to establish rules of conduct for all personnel involved in the design, development, operation, and maintenance of any Privacy Act system of records and